

# Android App for First Responders According to ISO/IEC 27037

Philipp Heischkamp, Fabian Adolphs

Aachen University of Applied Sciences

philipp.heischkamp@alumni.fh-aachen.de, adolphs@fh-aachen.de



IMF 2014

8TH INTERNATIONAL CONFERENCE ON IT SECURITY  
INCIDENT MANAGEMENT AND IT FORENSICS

- Preparation for the Workshop Activity
- IT First Responder Application
  - State of the Art
  - Challenges
  - Structure of ISO/IEC 27037:2012
  - Realization of the Android App
  - Conclusions
- Demo and Workshop Activity

# Preparation for the Workshop Activity

---

- Two options for you to use the IT First Responder Application

- Option 1: real App

- Smartphone (Android higher 3.0.0)



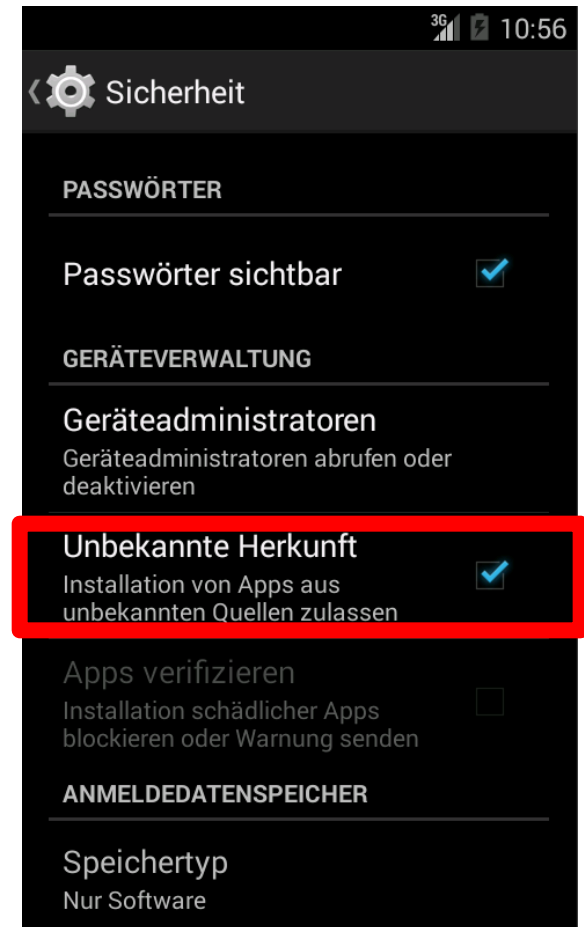
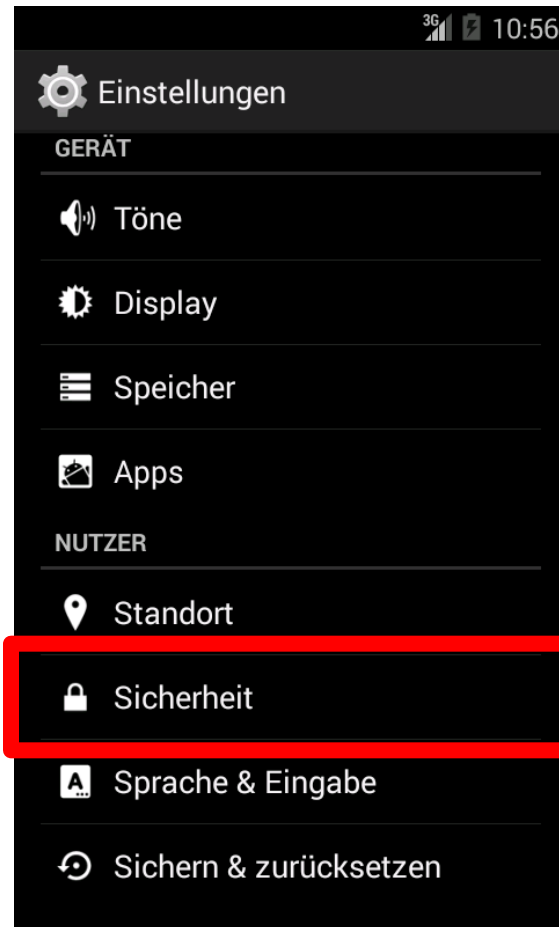
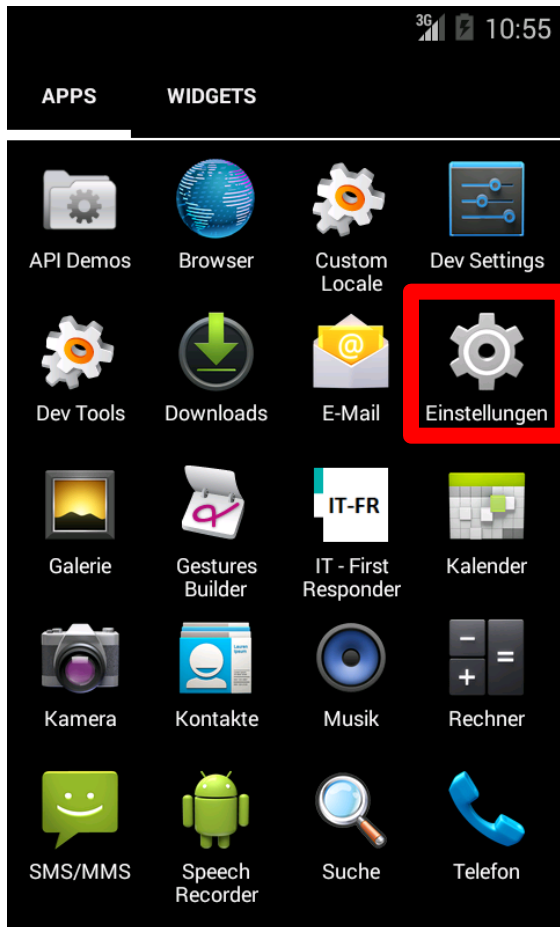
- Option 2: App in Emulator

- Laptop (Windows - 64 Bit)



# Preparation for the Activity (Android)

## 1. Activate "Unknown Applications"



# Preparation for the Activity (Android)

---

1. Activate "Unknown Applications"
2. Download App via Browser or QR-Tag
3. Install IT First Responder via download folder
4. Ready to use ...



[www.it-forensik.fh-aachen.de/  
images/download/  
FirstResponder/  
it-firstresponder.apk](http://www.it-forensik.fh-aachen.de/images/download/FirstResponder/it-firstresponder.apk)

- Tested on Galaxy: S, S2; Nexus: S; Moto: G;

# Preparation for the Workshop Activity

---

- Two options for you to use the IT First Responder Application

- Option 1: real App

- Smartphone (Android higher 3.0.0)



- Option 2: App in Emulator

- Laptop (Windows - 64 Bit)



# Preparation for the Workshop (Windows)

---

1. Open USB-Stick
2. Follow readme.txt instructions
  - (Modify parameters while copying and executing)
3. Ready to go ...



- Tested on a Windows 7 - 64 Bit System

# Agenda

---

- Preparation for the Workshop
- IT First Responder Application
  - State of the Art
  - Challenges
  - Structure of ISO/IEC 27037:2012
  - Realization of the Android App
  - Conclusions
- Demo and Workshop Activity



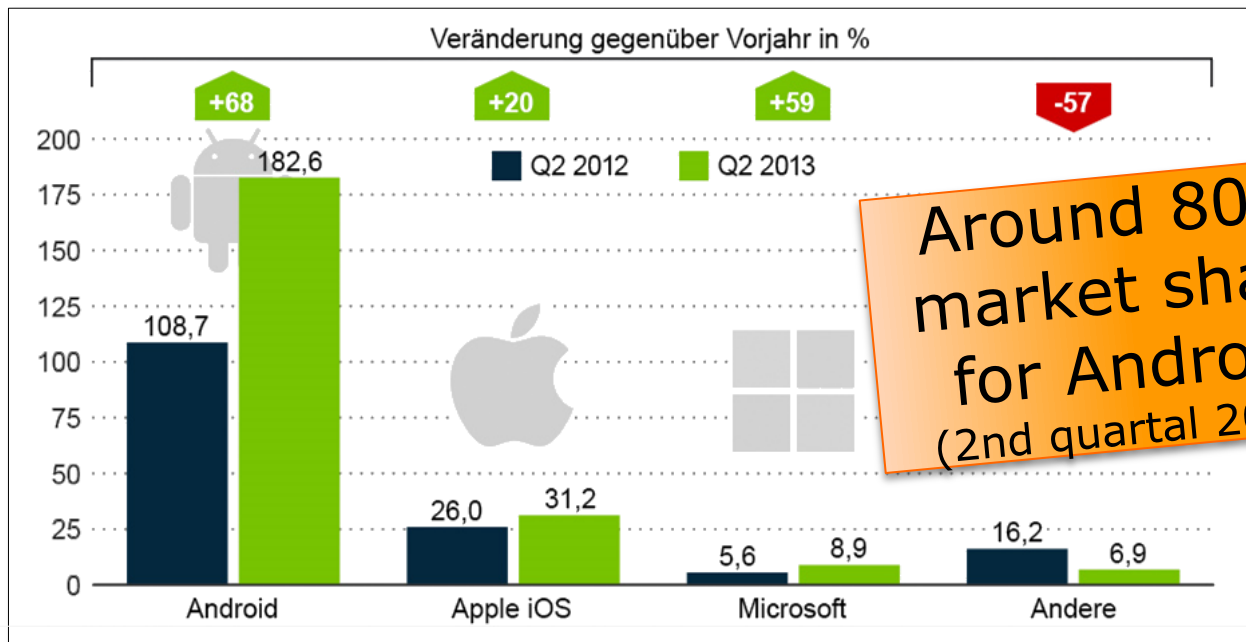
- Lots of different forensic tools for collection and analysis of digital evidence available
- ... but no tool that covers the procedure of a first response at an incident or crime scene
- Some guidelines exist for so-called Digital Evidence First Responders (DEFRR), e.g.
  - ISO/IEC 27037
  - „Leitfaden IT-Forensik“ from the BSI in Germany

BSI: Federal Office for  
Information Security

- Problems of textual guidelines
  - Lots of details (e.g. „Leitfaden IT-Forensik“ has more than 300 Pages)
    - including all non-relevant options for the case at hand
  - Inconvenient to be used in incident or crime scenes
    - “Hang on. I know I read this somewhere...”
  
- Idea
  - Implement ISO/IEC 27037:2012 as an interactive smart phone application
  - Guides DEFR through the process
  - Still: some prior training is needed

# Challenges

- Why an app?
  - Typical first responder probably owns a smart phone
  - Phone easy to transport (compared to a notebook)
  - Useful additional features (e.g. Camera)
  - Why Android? Well...



Quelle: Strategy Analytics

# Structure of ISO/IEC 27037:2012

---

- ISO/IEC 27037:2012 has 4 main sections:
  - General information and directives
  - Identification
    - Identification of affected devices
    - Documentation of items
  - Collection and acquisition
    - Gather items and copy data
    - Several decision trees for guidance
  - Preservation and transport
    - Guidelines for storage and transport of devices

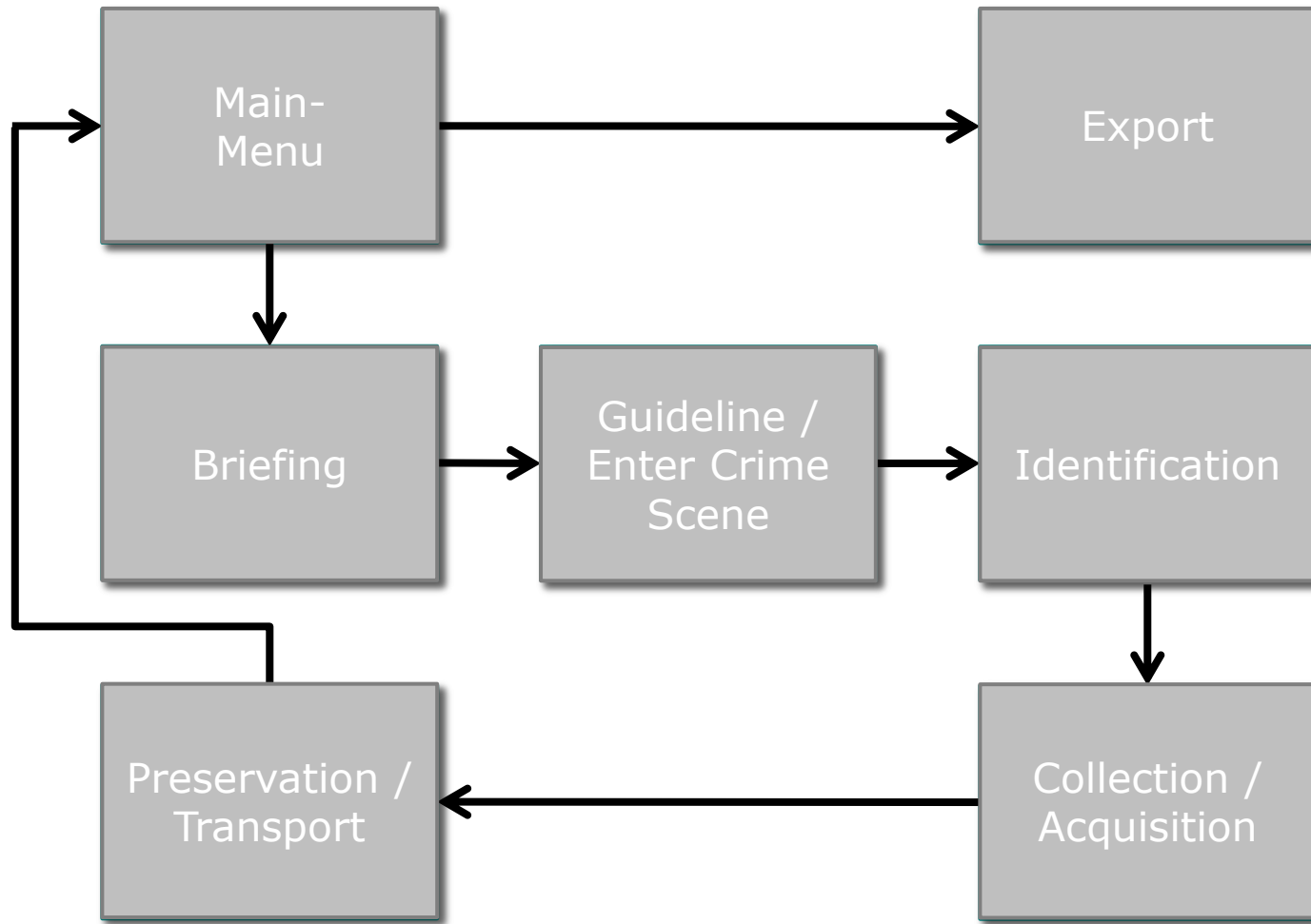
# Agenda

---

- Preparation for the Workshop
- IT First Responder Application
  - State of the Art
  - Challenges
  - Structure of ISO/IEC 27037:2012
  - Realization of the Android App
  - Conclusions
- Demo and Workshop Activity

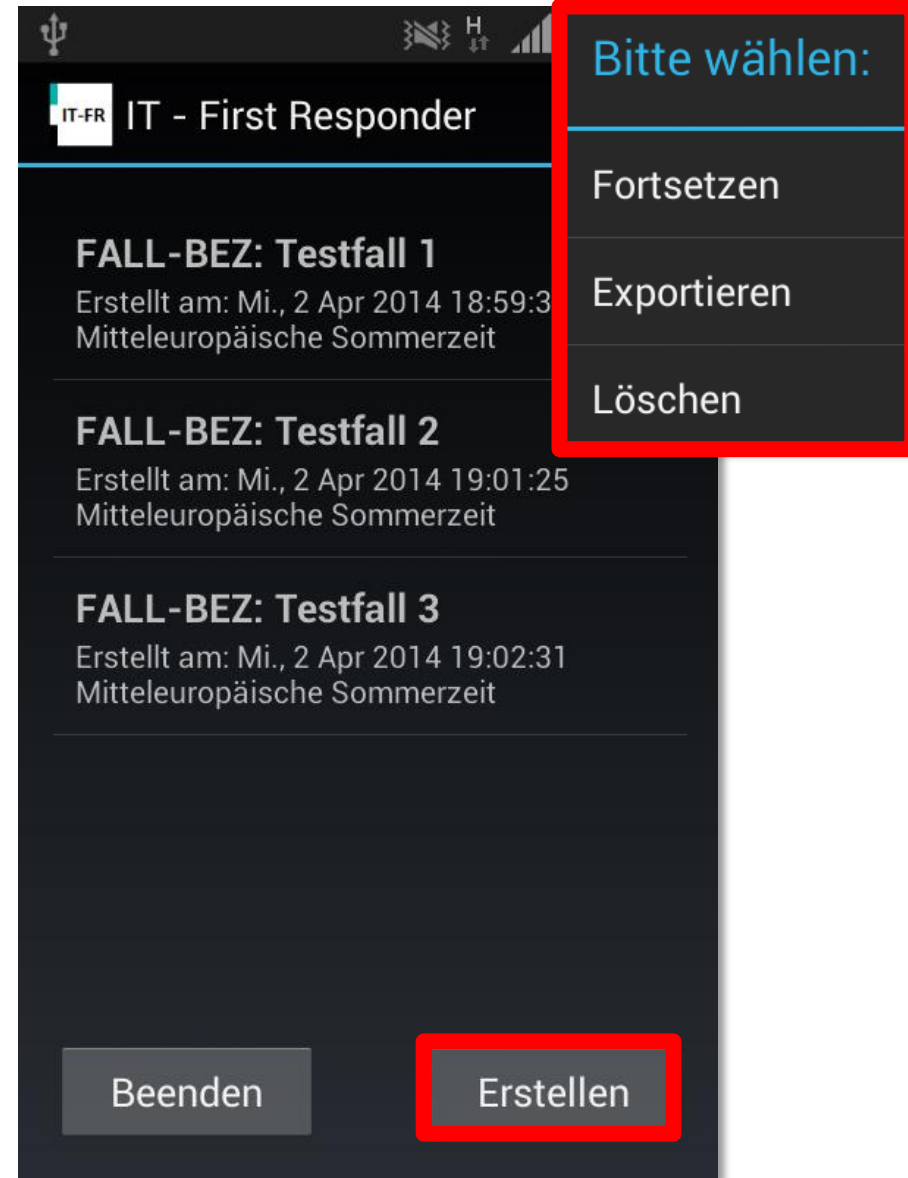
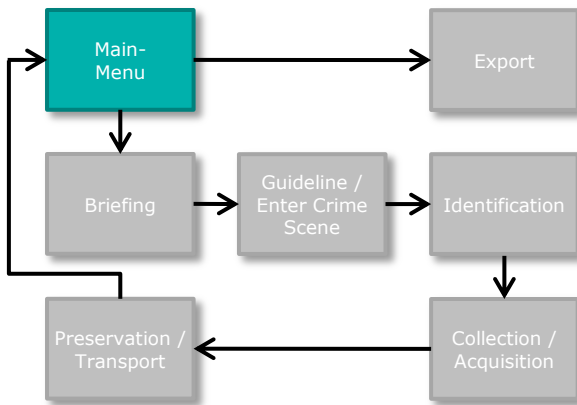
- Features of the Android Application
  - Implementation of ISO 27037
    - > by following the guidelines, it is ensured that the evidence can be used in court
  - Digital documentation of all actions
  - Smart phone camera for documentation
  - Creation of a final report including all data and pictures

# Realization of the Android App



# Realization of the Android App

- Main menu
  - Organisation of cases (e.g. continue, export, delete)
  - Creation of new cases

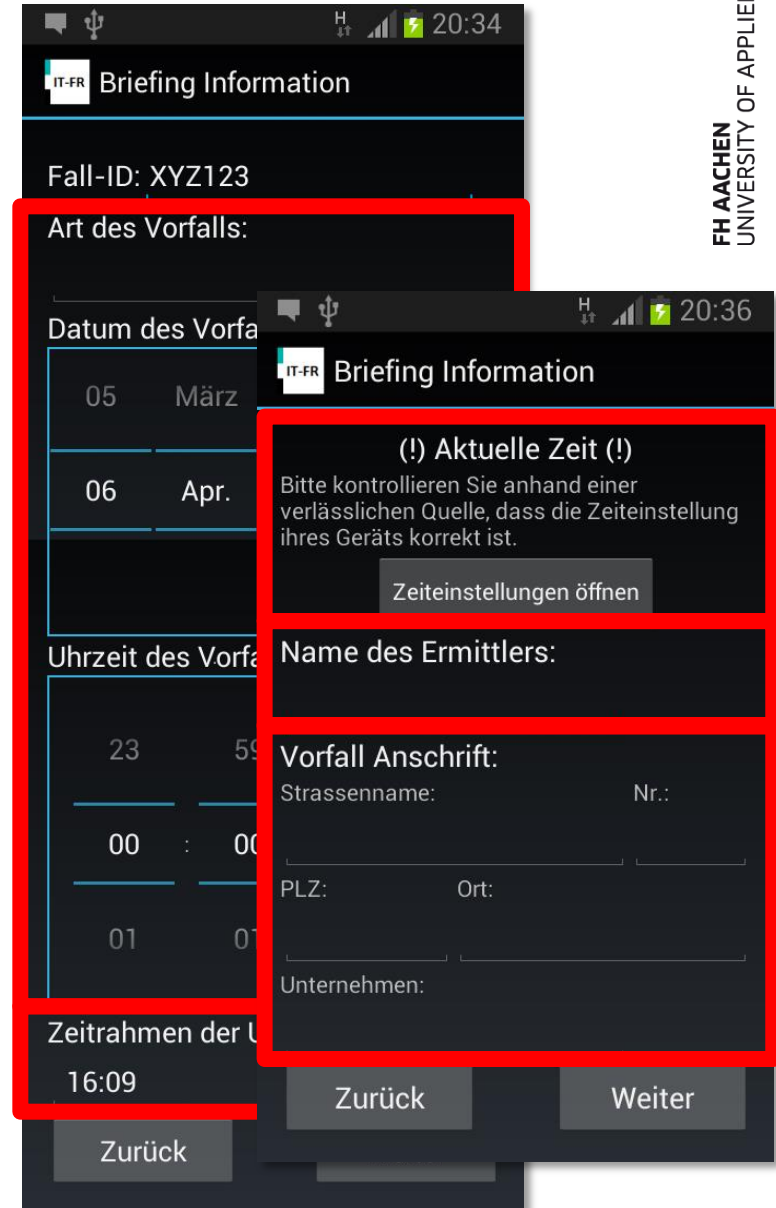
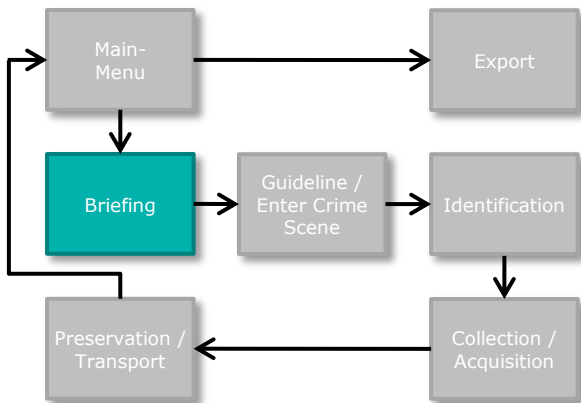




# Realization of the Android App


## ■ Briefing Information

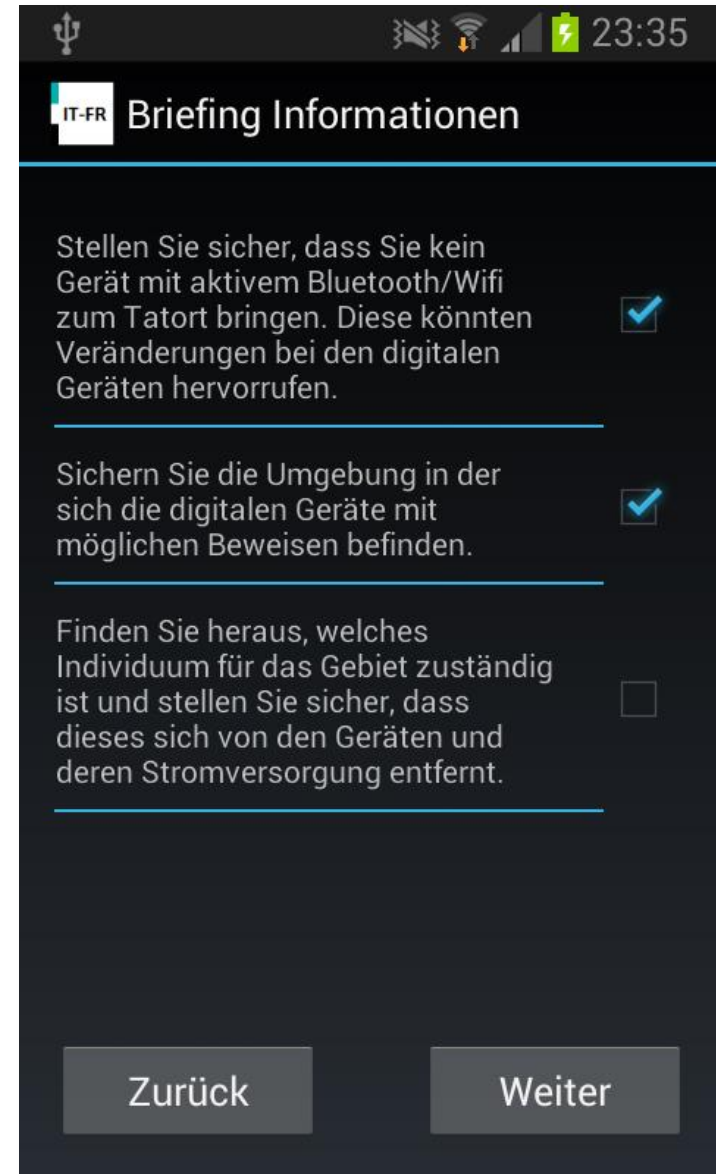
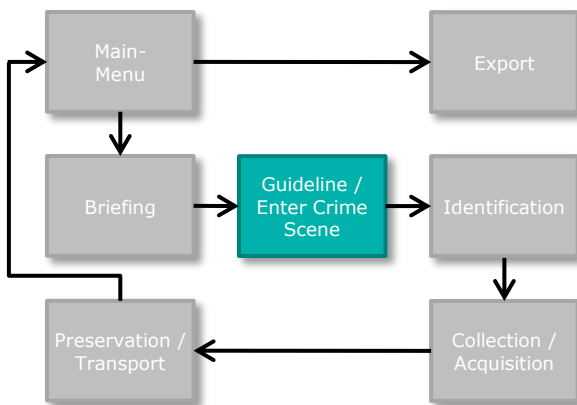
- Documentation of all case details
  - Case, date and time of incident
  - Time frame of investigation
  - Investigator
  - Address of incident
- Check of time/clock



# Realization of the Android App

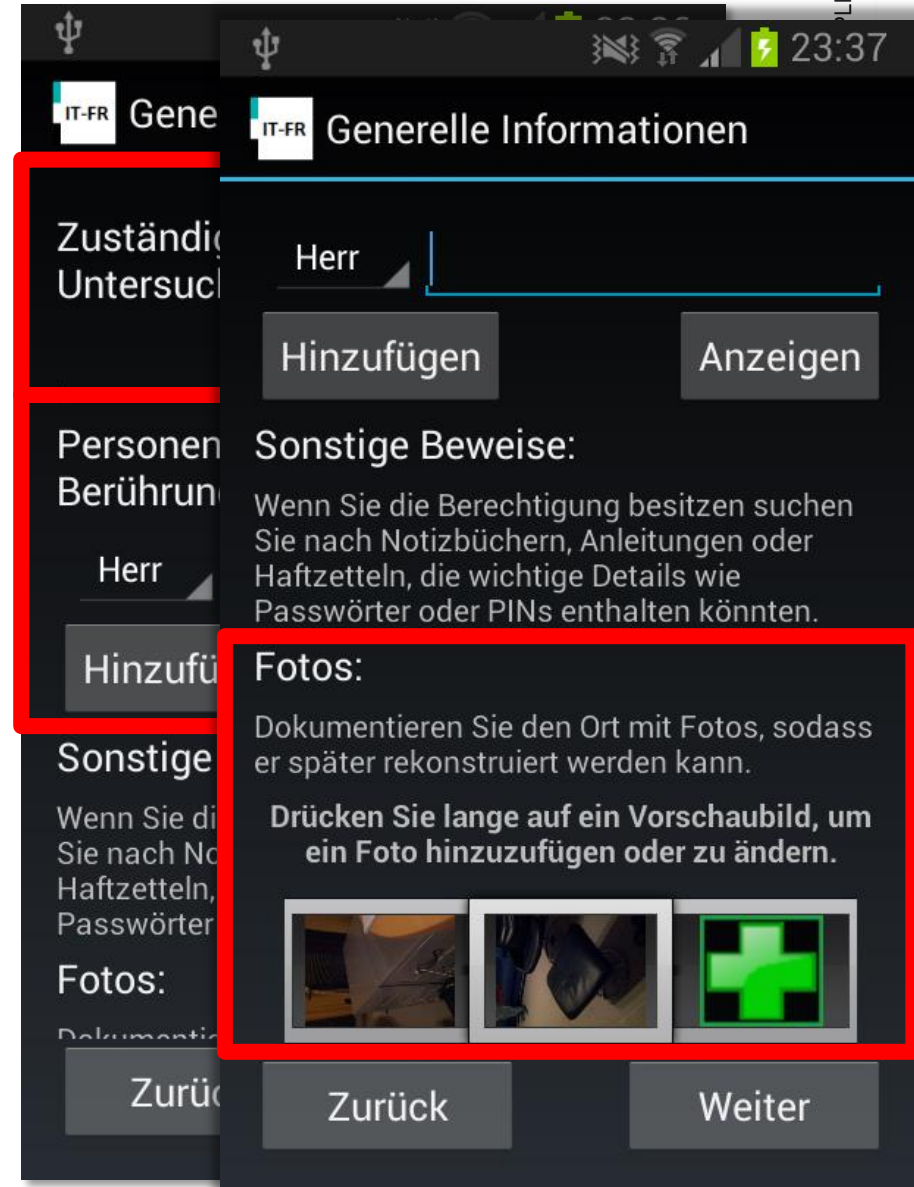
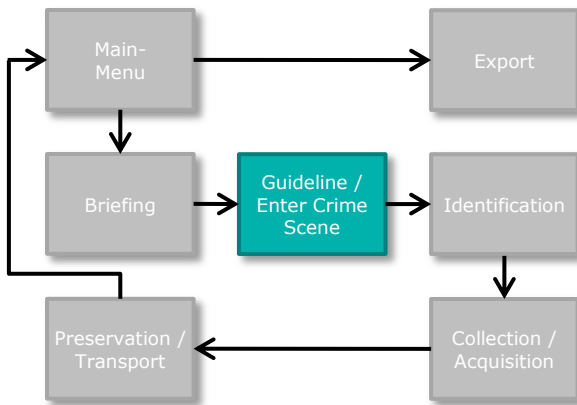
## ■ Guidance

- Briefing on appropriate handling of evidence
- Enforced through checkboxes 



# Realization of the Android App

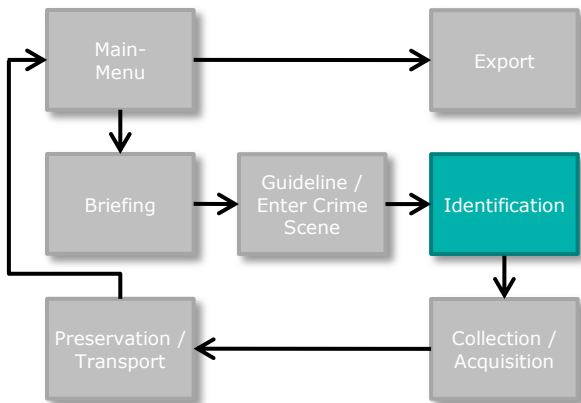
- Documentation of incident/crime scene
  - Responsible person on site
  - Persons, who got in touch with evidence
  - Pictures of scene for reconstruction purposes



# Realization of the Android App

## ■ Identification

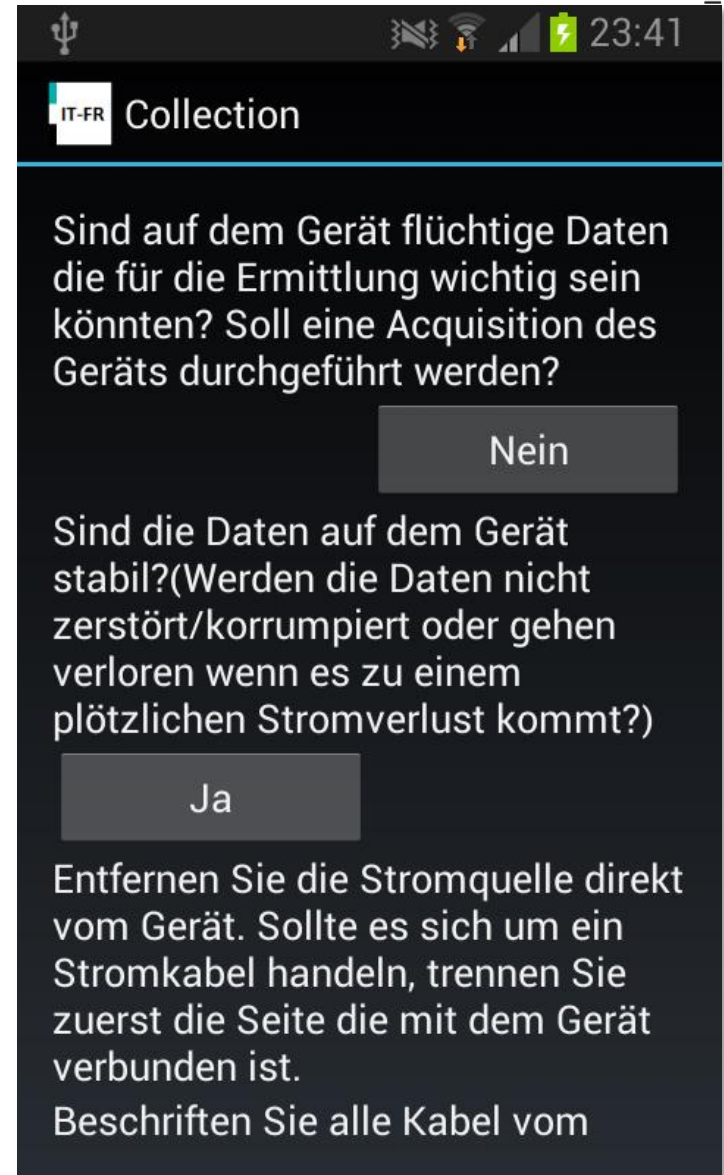
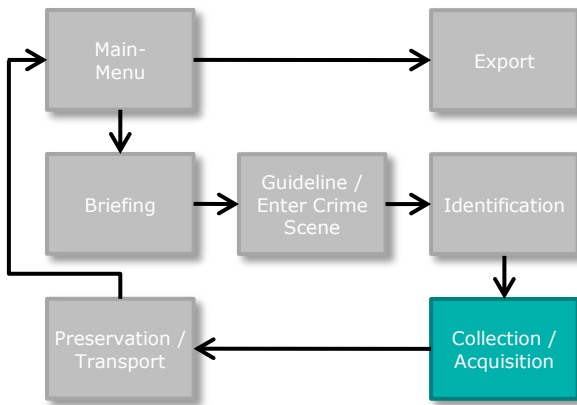
- Overview of all devices
- Identification dialog for every device
  - Description and type
  - Brand, serial and licence-key (optional by taking a picture)
  - Power and network state important for further processing
  - Pictures of devices (e.g. wiring)



The screenshot shows the 'Gerät hinzufügen' (Add Device) dialog in the app. The dialog is divided into several sections, with a red box highlighting the 'Gerät Bez. / Modell:' section and the 'Besondere Merkmale:' section. The 'Gerät Bez. / Modell:' section contains fields for 'Gerät Bez. / Modell:' (Testgerät 1), 'Typ:' (PC), 'Marke:' (Bild hinzugefügt), 'Seriennummer:' (Bild hinzugefügt), and 'Lizenznummer:' (XYZ1234567890). The 'Besondere Merkmale:' section contains a text field for 'Schäden, Aufkleber oder ähnliches.' and a list of checkboxes for 'Power an?' (checked) and 'Netzwerkverbindung vorhanden?' (unchecked). The 'Peripheriegeräte:' section contains a list of '1 Drucker'. The 'Fotos:' section contains buttons for 'Abbrechen' and 'Speichern'.

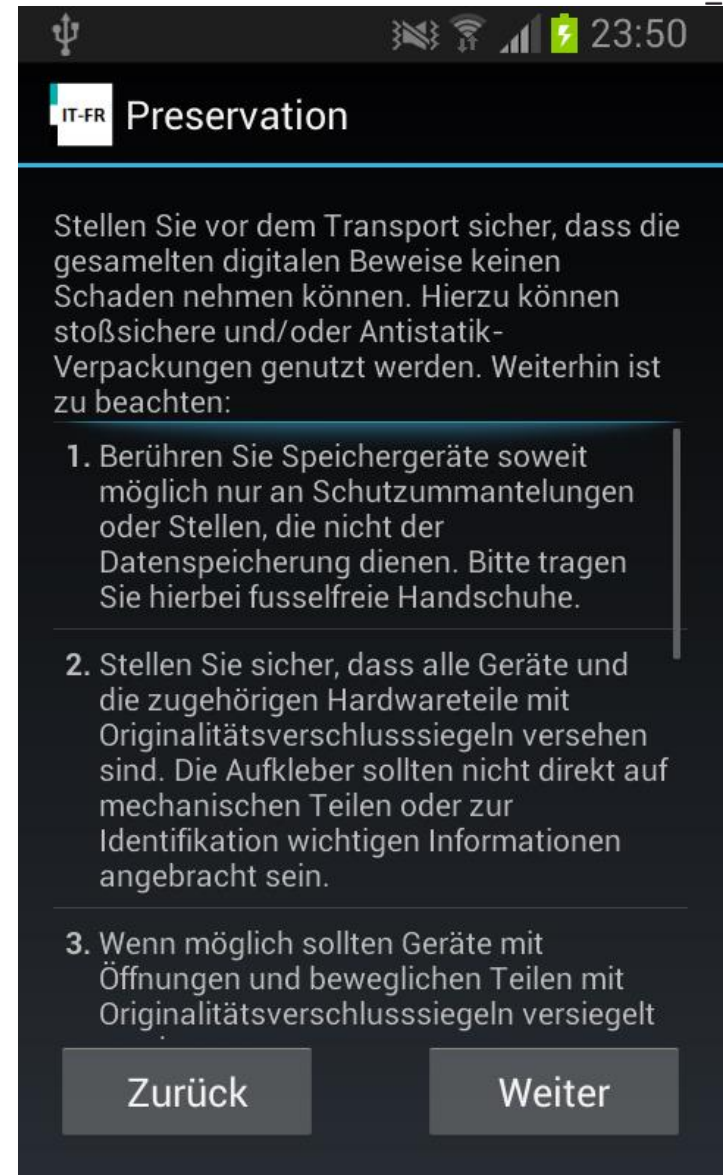
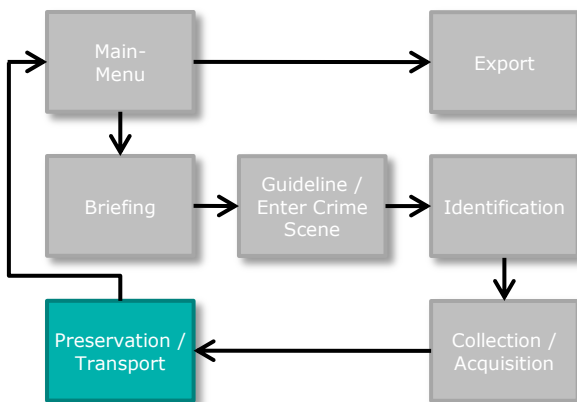
# Realization of the Android App

- Collection / Acquisition
  - Every device will be processed separately
  - Automatic guidance through ISO 27037 decision trees
  - Power and network state decides subsequent process steps
  - Special process for CCTV-Systems



# Realization of the Android App

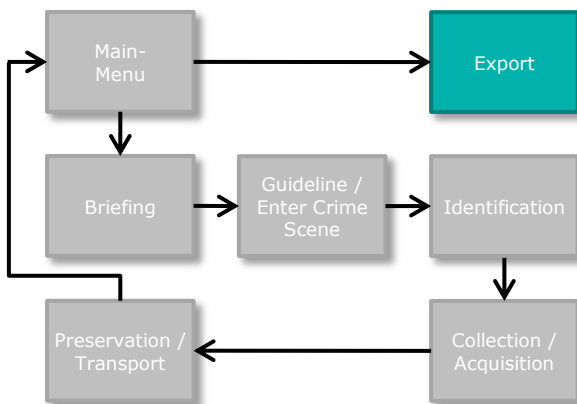
- Preservation / Transport
  - Detailed list as guideline to minimize risk of losing evidences
    - Wearing gloves
    - Preserving chain of custody



# Realization of the Android App

## ■ Export

- Automatic creation of a final report
  - HTML or XML
- Creation of SHA-256 hashes for every picture
- Automatic creation of a folder with all data (zip file)



# Realization of the Android App

## ■ Report

### Aufgenommene Geräte

Anzahl: 2

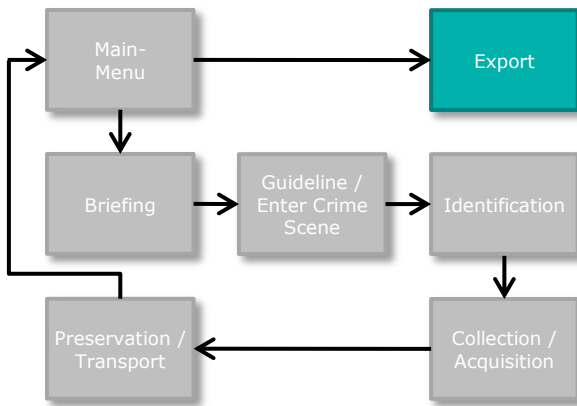
#### 1. Gerät: Testgerät 1

Eingetragen: Tue May 06 13:56:45 MESZ 2014

<b>Typ:</b>	PC
<b>Marke:</b>	IT_FirstResponder_29_20140506_135528.jpg
<b>Seriennummer:</b>	XYZ1234567890
<b>Lizenznummer:</b>	IT_FirstResponder_29_20140506_135544.jpg
<b>Netzwerkverbindung:</b>	Deaktiviert
<b>Power:</b>	An
<b>Merkmale:</b>	keine besonderen Merkmale
<b>Peripheriegeräte:</b>	
<b>Weiter bearbeitet:</b>	Tue May 06 13:58:05 MESZ 2014
<b>Weg der Bearbeitung:</b>	Es sind keine flüchtigen Daten auf dem Gerät für die eine Acquisition durchgeführt werden muss. --Die Daten auf dem Gerät sind nicht stabil und es kann, bei plötzlichem Stromverlust, zu Datenverlust kommen. --Das Gerät wurde ordnungsgemäß heruntergefahren. --Alle Kabel des Geräts wurden beschriftet und anschliessen entfernt. Tape wurde über den Stromschalter platziert um versehentliches verstellen zu verhindern. --CD/DVD/Disketten Laufwerke wurden (falls vorhanden) mit Tape verschlossen.

#### Gerät Fotos: 4

Dateiname	Aufnahmezeit
IT_FirstResponder_29_20140506_135528.jpg	Tue May 06 13:55:40 MESZ 2014
IT_FirstResponder_29_20140506_135544.jpg	Tue May 06 13:55:51 MESZ 2014
IT_FirstResponder_29_20140506_135625.jpg	Tue May 06 13:56:33 MESZ 2014
IT_FirstResponder_29_20140506_135636.jpg	Tue May 06 13:56:42 MESZ 2014





# Realization of the Android App

---

## ■ Application Facts

- Compatible for Android-Version  $\geq 3.0.0$ 
  - Covers 80% of all devices
- Easy to translate
  - English and German versions exist
- Size of app only 1,4 MB
  - Fast download



# Agenda

---

- Preparation for the Workshop
- IT First Responder Application
  - State of the Art
  - Challenges
  - Structure of ISO/IEC 27037:2012
  - Realization of the Android App
  - **Conclusions**
- Demo and Workshop Activity

# Conclusions

---

- User-friendly app for DEFRs
- App supports DEFR by
  - digital documentation
  - integrated usage of camera function
  - automatic creation of a report
- Guidance on a case by case basis
  - based on DEFR input appropriate steps are selected

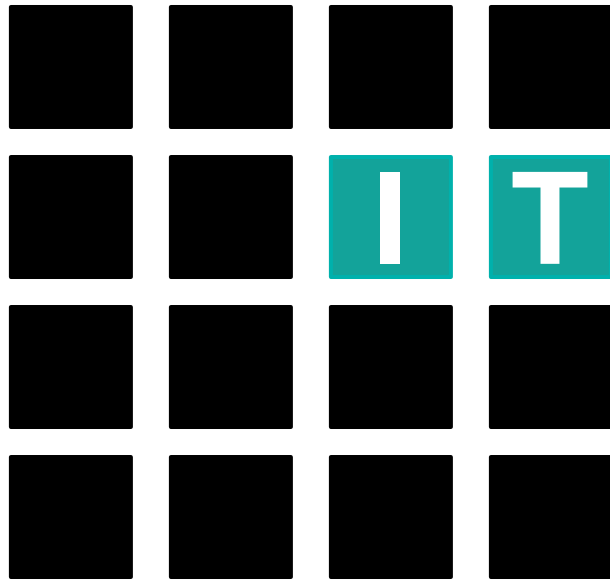
# Agenda

---

- Preparation for the Workshop
- IT First Responder Application
  - State of the Art
  - Challenges
  - Structure of ISO/IEC 27037:2012
  - Realization of the Android App
  - Conclusions
- Demo and Workshop Activity

- Example Case

- Your neighbour is suspected to send malicious software from her / his notebook
- Use the app to document the incident
- But please:
  - Do not start a live response (no RAM images or similar)
  - No screw drivers
- Just document the case from the outside...



# Forensics

@ FH Aachen

**Thank you!**  
**Any Questions?**

Fabian Adolphs

(adolphs@fh-aachen.de)

<http://www.it-forensik.fh-aachen.de/projekte/itfirstresponder>